



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/754,713	01/12/2004	Jason Whitman Keith Brothers	23415-027	1344

909 7590 04/19/2007
PILLSBURY WINTHROP SHAW PITTMAN, LLP
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER

PALIWAL, YOGESH

ART UNIT	PAPER NUMBER
----------	--------------

2109

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/754,713

Applicant(s)

KEITH BROTHERS ET AL.

Examiner

Yogesh Paliwal

Art Unit

2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-30 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) ____ is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 12 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: ____.

DETAILED ACTION

Claim Objections

Claim Objections - 37 CFR 1.75(a)

1. The following is a quotation of 37 CFR 1.75(a):

The specification must conclude with a claim particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention or discovery.

Claims 28 and 29 are objected to under 37 CFR 1.75(a), as failing to particularly point out and distinctly claim the subject matter which application regards as his invention or discovery.

Claims 28 and 29 both depend from claim 23 and recite a limitation "wherein the fourth module block", which lacks antecedent basis. By referring back to claim 23, it appears that "third module" actually block data packets. This appears to be a typographical error. In light of the corresponding written description of the invention, and for purposes of examination, "forth module" will be replaced with "third module" in both claims 28 and 29. Clarification is required.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Art Unit: 2109

The USPTO "Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility" (Official Gazette notice of 22 November 2005), Annex IV, reads as follows:

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).) "Nonfunctional descriptive material" includes but is not limited to music, literary works and a compilation or mere arrangement of data.

When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized. Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994) (claim to data structure stored on a computer readable medium that increases computer efficiency held statutory) and *Warmerdam*, 33 F.3d at 1360-61, 31 USPQ2d at 1759 (claim to computer having a specific data structure stored in memory held statutory product-by-process claim) with *Warmerdam*, 33 F.3d at 1361, 31 USPQ2d at 1760 (claim to a data structure per se held nonstatutory).

In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. See *Lowry*, 32 F.3d at 1583-84, 32 USPQ2d at 1035.

Claims **16-22** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows. Claims 16-22 define a "computer program product" embodying functional descriptive material. However, the claim does not define a computer-readable medium or memory and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized" – Guidelines Annex IV). That is, the scope of the presently claimed "computer program product" can range from paper on which the program is written, to a program simply contemplated and memorized by a person. The examiner suggests amending the claim to embody the program on "computer-readable

Art Unit: 2109

medium" or equivalent in order to make the claim statutory. Any amendment to the claim should be commensurate with its corresponding disclosure.

Claims **10-15** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter as follows. Although Claims 10-15 are directed towards "system for protecting a computer network", the specification provides intrinsic evidence that these claims are directed towards software alone. System as claimed in claims 10-15 is nothing more than software modules performing different tasks of the overall software module.

Claims 10-15 define systems embodying functional descriptive material. However, the claims do not define a computer-readable medium or memory and is thus non-statutory for that reason (i.e., "When functional descriptive material is recorded on some computer-readable medium it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized" – Guidelines Annex IV). That is, the scope of the presently claimed systems of claims 10-15 can range from paper on which the program is written, to a program simply contemplated and memorized by a person. The examiner suggests amending the claim to embody the program on "computer-readable medium" or equivalent in order to make the claim statutory. Any amendment to the claim should be commensurate with its corresponding disclosure.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims **1-7, 10, 12-14, 16-20, 23, 25-28** are rejected under 35 U.S.C. 102(e) as being anticipated by Shetty (US 6,772,345).

Regarding **Claims 1, 10 and 16**, Shetty discloses a method, system and computer program product of monitoring network communications for an indication of an attack and disabling the network communications upon an existence of a predetermined condition (**Column 1, lines 6-8, “The present invention relates to a method, system and computer program product for detecting computer malwares that scans network traffic at the protocol level”**), comprising:

monitoring data packets received at a target system in real time (**Column 1, lines 58-60, “Malware scanning of data that is being transferred or downloaded to a computer system”**) ;

Art Unit: 2109

identifying the received data packets that are associated with signatures of the attack (**Column 1, lines 65-66, “Scanning the data stream at a protocol level to detect a malware”**);

determining a severity of the attack; and blocking the data packets from entering the target system when the severity of the attack exceeds a predetermined threshold (**Column 5, lines 5-8 “All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria”**)

Regarding **Claim 2 and 12**, rejection of claims 1 and 10 is incorporated and further Shetty discloses that the data packets received at the target system are monitored based on at least one of identifying information and a type of communication (**Column 3 lines 13-17, “As shown in FIG. 1, incoming network traffic 102 and outgoing network traffic 104 are filtered by one or more protocol filters, such as filters 106A-C. The protocol filters scan the traffic data stream for malwares”**)

Regarding **Claim 3**, rejection of claim 2 is incorporated and further Shetty discloses that the identifying information includes at least one of an Internet Protocol address and a port number (**Column 3, lines 56-57,61 and Column 4 line 1, “Preferably, protocol scanner 108 will be capable of performing a number of function:” ... “Blocking an IP address or set of IP address” ... “Blocking ports”**)

Art Unit: 2109

[Shetty's system is capable of blocking incoming packets based on the source IP address or just block traffic on certain ports]

Regarding **Claim 4**, rejection of claim 2 is incorporated and further Shetty discloses that the type of communication includes at least one of a File Transfer Protocol, a Simple Mail Transfer Protocol, Telnet, Domain Name System, Windows Internet Name System, HyperText Transfer Protocol, Traceroute, instant messaging, and chat (**Column 3, lines 21-28, "Filter functionality is required for each protocol that is to be supported. For example, Post Office Protocol 3 (POP3) filter 106A scans the POP3 data stream, HyperText Transfer Protocol (HTTP) filter 106B scans the HTTP data stream, and File Transfer Protocol (FTP) filter 106C scans the FTP data stream. POP3 is a protocol used to retrieve e-mail from a mail server, HTTP is the underlying protocol used by the World Wide Web, and FTP is a protocol used on the Internet for sending files"**)

Regarding **Claim 5**, rejection of claim 1 is incorporated and further Shetty discloses that the data packets received at the target system are monitored using Transmission Control Protocol/Internet Protocol at an application layer (**Column 3, lines 58-60, "Scanning for computer malwares, such as viruses, Trojans and worms in the entire network TCP/IP protocol like HTTP, FTP, SMTP/POP3, etc."**)

Art Unit: 2109

Regarding **Claim 6, 13 and 19**, rejection of claims 1,10 and 16 is incorporated and further Shetty discloses that the severity of the attack is determined based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, and a volume of received data packets (**Column 3, lines 65-67, “Blocking emails (stop network spamming): by scanning POP3 and SMTP protocols, protocol scanner 108 will be able to block emails from specified addresses.”**) [*This is a detection of the severity of the attack based on a type of communication i.e. blocking emails from specified addresses*]

Regarding **Claim 7,14 and 20**, rejection of claim 1, 10 and 16 is incorporated and further Shetty discloses that the data packets are blocked from entering the target system by instructing at least one of a router, a hub, a server, and a firewall to disable a communication channel (**Column 5, lines 5-8 “All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria”**)

Regarding **Claim 17**, rejection of claim 16 is incorporated and further Shetty discloses that the received data packets are monitored transparently in real-time (**Column 1, lines 58-60, “Malware scanning of data that is being transferred or downloaded to a computer system”**) [It can be seen that security configuration of Shetty’s system that includes router/firewall and gateway system that is responsible for scanning incoming data is transparent to both the data receiving and sending host]

Regarding **Claim 18**, rejection of claim 16 is incorporated and further Shetty discloses that the received data packets are monitored after being stored in a storage buffer (**Column 7, lines 22-27, “Memory 408 includes protocol scanner 410, which includes at least one protocol filter, such as protocol filters 412A and 412B, application programs 414, and operating system 412. Protocol scanner 410 scans for network traffic for malwares and then forwards the scanned data to workstation computers and/or workstation computer applications”**)

Regarding **Claim 23**, Shetty discloses a system configured to monitor data packets received on a transmission medium for an indication of an attack and to block receipt of the data packets upon an existence of a predetermined condition (**Column 1, lines 6-8, “The present invention relates to a method, system and computer program product for detecting computer malwares that scans network traffic at the protocol level”**), comprising:

- at least one terminal device (**Figure 3, Numeral 312A, “WORKSTATION”**);

- an application server that is coupled to the at least one terminal device for processing requests sent by the at least one terminal device (**Figure 3, Numeral 308, “GATEWAY”**);

- a monitoring server that is coupled to the application server for monitoring data packets (**Figure 3, Numeral 310, “PROTOCOL SCANNER”**),

- the monitoring server having one or more modules comprising:

Art Unit: 2109

a first module that receives attack signatures associated with data packets and monitors received data packets for the attack signatures (**Column 1, lines 58-60, “Malware scanning of data that is being transferred or downloaded to a computer system”**) ;

a second module that evaluates the received data packets having the attack signatures and determines a severity of an attack on the computer system (**Column 1, lines 65-66, “Scanning the data stream at a protocol level to detect a malware”**); and

a third module that identifies a source of the attack and instructs at least one switching device to block the data packets associated with the attack signatures if the severity of the attack exceeds a predetermined threshold (**Column 5, lines 5-8 “All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria”**).

Regarding **Claim 25**, rejection of claim 23 is incorporated and further Shetty discloses a database coupled to the monitoring server (**Column 3, lines 61-67 and Column 4, lines 1-13**) [*Since the protocol scanner is capable of blocking data based on IP address or specific e-mail address, specific block and specific URLs, then it must have a database with all the entries of the IP addresses, e-mail address, port numbers and URLs to block*]

Regarding **Claim 26**, rejection of claim 23 is incorporated and further Shetty discloses that the first module is adapted to monitor the received data packets based on at least one of identifying information and a type of communication (**Column 3 lines 13-17, “As shown in FIG. 1, incoming network traffic 102 and outgoing network traffic 104 are filtered by one or more protocol filters, such as filters 106A-C. The protocol filters scan the traffic data stream for malwares”**).

Regarding **Claim 27**, rejection of claim 23 is incorporated and further Shetty discloses that the third module is adapted to determine the severity of the attack based on at least one of a frequency of the attack, a type of communication, a change in an amount of bandwidth, and a volume of received data packets (**Column 3, lines 65-67, “Blocking emails (stop network spamming): by scanning POP3 and SMTP protocols, protocol scanner 108 will be able to block emails from specified addresses.”**) [*This is a detection of the severity of the attack based on a type of communication i.e. blocking emails from specified addresses*].

Regarding **Claim 28**, rejection of claim 23 is incorporated and further Shetty discloses that the fourth module blocks data packets from entering the computer network by instructing at least one of a router, a hub, a server, and a firewall to disable a communication channel (**Column 5, lines 5-8 “All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria”**).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 8, 21 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shetty (US 6,772,345) in combination with a suggestion from the same reference.

Regarding **Claim 8, 21 and 30**, rejections of claims 1, 16 and 23 are incorporated and Shetty does not explicitly teaches the step of notifying an attacking source of a detection of the attack and of blocking the data packets sent from the attacking source.

However, Shetty in the background section of the reference discloses a step of notifying an attacking source of a detection of the attack and of blocking the data packets sent from the attacking source (**Column 1, lines 32-34, "The anti-virus program may then take corrective action, such as notifying a user or administrator of the computer system of the virus"**)

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to notify a user or administrator of the virus source computer as taught by the background section of Shetty, after detecting and blocking the virus in Shetty's system *so that the administrative or user of the source computer from where the virus was generated can take corrective action to clean his/her system or to let*

Art Unit: 2109

him/her know why the connection is refused or blocked by router/firewall of the target system.

Claims 9, 11, 15, 22, 24 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shetty (US 6,772,345) in view of Lachman, III et al. (US 2002/0166063).

Regarding **Claims 9, 15, 22 and 29**, rejections of claims 1,14,16 and 23 are incorporated and further Shetty teaches blocking data packets. He does not teach blocking data packets from entering the target system for a predetermined amount of time only.

However, Lachman, III et al., in the same field of endeavor of network security, discloses the data packets are blocked from entering the target system for a predetermined amount of time (Paragraph 0125, "If the flooding is of the single-source type, no packets will be routed from that source to the victim IP address for the specified block time).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to block the data packets as disclosed by Shetty for only a predetermined amount of time as taught by Lachman, III et al. to *"prevent network flood interruptions without disrupting normal network operations"* (Paragraph 0002, Lachman, III et al.)

Regarding **Claims 11 and 24**, rejections of claims 10 and 23 are incorporated and Shetty doesn't disclose comprising a log-creating module that is adapted to create a log of the received data packets having the attack signatures.

However, Lachman, III et al. further discloses a log-creating module that is adapted to create a log of the received data packets having the attack signatures **(Paragraph 0105, "if the network load reaches the set threshold, then system 106 can launch a countermeasure routine and can log the time of the flood, the time of the countermeasure deployment, and the source and destination of the offending packet (s).")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to create a log, as taught by Lachman, III et al., of the received data packets having the attack signature in the system of Shetty so that *the source of the offending packet (Lachman, III et al., Paragraph 0105) can be added to the blocking list of Shetty's router/firewall so that "the source will not [be] able to send or receive any data from the protected corporation network" (Shetty, Column 3, lines 62-64)*

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.


Art Unit: 2109

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian P. Werner can be reached on (571) 272-7401. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



YP
4/09/2007



BRIAN WERNER
SUPERVISORY PATENT EXAMINER